

**REMARKS/ARGUMENTS**

Upon entry of the present amendment, claims 1, 2, and 4-20 remain pending in this application, of which claims 1, 4, 5, 11, 14, 16, and 17 are amended. Claim 3 has been cancelled. Applicants respectfully submit that that no new matter has been added by the present amendment. Claim 16 stands rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicant regards as his invention. Claims 1, 2, 7, and 9 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 6,167,517 ("Gilchrist"). Claims 3-6, 8, 10-13, 17, and 20 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Gilchrist in view of U.S. Patent No. 6,310,966 ("Dulude") and further in view of U.S. Patent No. 5,280,527 ("Gullman"). Claims 14-16, 18, and 19 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Gilchrist in view of Dulude and Gullman and further in view of U.S. Patent No. 6,092,201 ("Turnbull"). Applicant respectfully requests reconsideration of the present application in light of the below recited remarks.

***Rejections Under 35 U.S.C. § 112***

Claim 16 stands rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicant regards as his invention. Claim 16 is amended to provide antecedent basis for the limitations "server" and "the server".

***Rejections Under 35 U.S.C. § 102(e)***

Claims 1, 2, 7, and 9 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 6,167,517 ("Gilchrist"). Applicant respectfully disagrees.

Independent claim 1 includes a feature neither taught nor suggested by the prior art, namely: "a security code generator coupled to [a] sensor to sign the biometric data with a signature corresponding to the sensor."

The present invention is directed to systems and methods for securely transmitting and authenticating biometric data over a network. More specifically, there is disclosed:

“[w]e prefer to provide a camera which functions as a sensor to collect the biometric data. That data is digitized into a biometric data file. A code is applied to that file. Then the file with code is output to a network for transfer to an authentication server system. The authentication server system validates the data by re-computing the code from its knowledge of the input data needed to generate that code. If the data is authenticated, the server distills the biometric data file into a biometric template for use in verifying the identity of the user (Application, Summary of the invention).”

Gilchrist discloses systems and methods for trusted biometric authentication.

Gilchrist discloses that:

“[a] host system receives an identifier for the user from a client system. This identifier is used to retrieve a template containing biometric data associated with a user, and this template is returned to the client. The client then gathers a biometric sample from the user, and compares this biometric sample with the template to produce a comparison result. Next, the client computes a message digest using the template, the comparison result and an encryption key, and sends the message digest to the host system. This computation takes places within a secure hardware module within the client computing system that contains a secure encryption key in order to guard against malicious users on the client system. Next, the host system receives the message digest and authenticates the user by determining whether the message digest was computed using the template, the encryption key, and a comparison result indicating a successful match between the biometric sample and the template (Gilchrist, Col. 2, lines 27-45).”

Thus, Gilchrist discloses sending a data package including a biometric comparison result from a client to a host.

Importantly, and in contrast to the claimed invention, Gilchrist does not teach, “a security code generator coupled to [a] sensor to sign . . . biometric data with a signature corresponding to the sensor”, as recited in newly amended claim 1. *As noted by the Examiner, “Gilchrist however does not disclose ‘signing [a] biometric sample at the imaging device’ (Office Action, Page 5, Lines 4-5).”*

Applicant respectfully submits that dependent claims 2, 7, and 9 are patentable at least by reason of their dependency. Accordingly, reconsideration and withdrawal of the 35 U.S.C. § 102(e) rejections are respectfully requested.

*Rejections Under 35 U.S.C. § 103(a)*

**Claims 3-6, 8, 10-13, 17, and 20**

Claims 3-6, 8, 10-13, 17, and 20 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Gilchrist in view of Dulude and further in view of Gullman.

Applicant respectfully disagrees.

Independent claim 11 includes a feature neither taught nor suggested by the prior art, namely: “a code generator to generate a digital signature corresponding to the imaging device.”

Independent claim 17 includes features neither taught nor suggested by the prior art, namely: “authenticating [a] server at the imaging device; signing [a] biometric sample at the imaging device with a signature *corresponding to the imaging device*; and *authenticating the imaging device* at the server.”

Gilchrist discloses sending a data package including a biometric comparison result from a client to a host (Gilchrist, Summary of the Invention).

Dulude discloses encrypting transaction data and a user's sample biometric data with the user's private key and transmitting the encrypted data from a sending device to a receiving device. At the receiving device, the encrypted data may be decrypted and the user's identity may be authenticated using the user's pre-stored biometric data (Dulude, Summary of the Invention).

Gullman discloses the use of a biometric token for authorizing access to a host system. The token includes a comparison between a biometric input from a user and a template (Gullman, Summary of the Invention).

Importantly, the cited references, taken alone or in combination, do not teach signing biometric data with a signature of an imaging device and authenticate the imaging device with such a signature, as recited by the claims of the present application. However, the Examiner states that, Dulude teaches, “a digital signature function, in which [biometric data] is signed; that is, encrypted using the private key of the first user (Office Action, Page 5, Paragraph 2)”. Applicant respectfully submits that *encrypting* biometric data with a private key of *a user* is not similar to *signing* biometric data with a signature of *an imaging device*. Encrypting biometric data with a private key of a user *merely secures transmission and does*

*not authenticate the imaging device.* Authentication of the imaging device is desirable because a user may submit a forged or inaccurate biometric sample using a non-authenticated imaging device. Furthermore, although Dulude discloses that a user's identity may be authenticated by comparing biometric samples (Dulude, Col. 7, lines 26-28), Applicant respectfully submits that authenticating a user's identity is not similar to authenticating an imaging device.

Specifically, with respect to independent claim 1, Dulude and Gullman do not cure the deficiencies of Gilchrist because neither Dulude nor Gullman teach, "a security code generator coupled to [a] sensor to sign [the] biometric data with a signature *corresponding to the sensor*", as recited in the claim. Furthermore, with respect to independent claim 11, the cited references do not teach, "a code generator to generate a digital signature *corresponding to the imaging device*", as recited in the claim. Additionally, with respect to independent claim 17, the cited references do not teach, "authenticating [a] server at the imaging device; signing [a] biometric sample at the imaging device with a signature *corresponding to the imaging device*; and *authenticating the imaging device* at the server", as recited in the claim.

Applicant respectfully submits that dependent claims 4-6, 8, 10, 12, 13, and 20 are patentable at least by reason of their dependency.

#### **Claims 14-16, 18, and 19**

Claims 14-16, 18, and 19 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Gilchrist in view of Dulude and further in view of Gullman and further in view of Turnbull. Applicant respectfully disagrees.

Independent claim 14 includes a feature neither taught nor suggested by the prior art, namely: "signing the biometric data with the imaging device private key."

Turnbull discloses that a receiving party may authenticate a public key of a sending party by using the sending party's signature public key certificate obtained from a certification authority (Turnbull, Col. 1, line 64 - Col. 2, line 2). Importantly, neither Turnbull nor the other cited references teach signing biometric data with a signature of an *imaging device*, as disclosed in the claims of the present application.

Specifically, with respect to newly amended independent claim, 14 the cited references do not teach, "signing . . . biometric data with the imaging device private key", as

DOCKET NO.: IRID-0479  
Application No.: 10/020,791  
Office Action Dated: June 24, 2003

PATENT

recited in the claim. Additionally, with respect to independent claim 17, the cited references do not teach, “authenticating [a] server at the imaging device; signing [a] biometric sample at the imaging device with a signature *corresponding to the imaging device*; and *authenticating the imaging device* at the server”, as recited in the claim.

Applicant respectfully submits that dependent claims 15, 16, 18, and 19 are patentable at least by reason of their dependency. Accordingly, reconsideration and withdrawal of the 35 U.S.C. § 103(a) rejections are respectfully requested.


**DOCKET NO.:** IRID-0479  
**Application No.:** 10/020,791  
**Office Action Dated:** June 24, 2003

**PATENT**

**CONCLUSION**

In view of the above remarks, Applicant respectfully submits that the present application is in condition for allowance. Reconsideration of the application and an early Notice of Allowance are respectfully requested.

Date: September 22, 2003

  
\_\_\_\_\_  
Kenneth R. Eiferman  
Registration No. 51,647

Woodcock Washburn LLP  
One Liberty Place - 46th Floor  
Philadelphia PA 19103  
Telephone: (215) 568-3100  
Facsimile: (215) 568-3439